

Gray Pixel Value based Vein Feature Extraction and Recognition on FPGA

Savitha A. P
Research Scholar
Viswesharaya Technological University
Belagaum-590001
Karnataka, India

Dr. Ramegowda
Professor
Rajeev Institute of Technology
Hassan-573201
Karnataka, India

Abstract— The proposed paper presents a new technique in the authentication system in contactless palm vein biometric modality. This work is focused on improving the security and performance of a palm vein pattern recognition system. This work is dedicated to verifying an efficient and robust authentication system on a field-programmable gate array (FPGA). The proposed method is carrying at three different levels. (1) Palm vein image feature (Gray value) detection and extraction (2) A secrete key generation using 16-bit Cyclic Redundancy check (CRC) checksum. (3) Realization and implementation of level (1) and (2) on FPGA. Level (3) describes the verification and validation of the palm vein features on FPGA. The state-of-the-art of the proposed work is to design and implement a 2-level palm vein authentication system (PVAS) by adapting CRC to ensure proper encoding and decoding of the data. The implementation result of PVAS on FPGA shows a faster time of 1.979000ns for data validation process and accuracy of 98.921%. The objective of the present work is to analyze and compare system performance on software and hardware platform. Finally, it observed from the result that CRC-16 is a highly secured algorithm for faster verification and validation of the system on FPGA.

Keywords— CRC, encoding, decoding, FPGA, minutiae detection, minutiae extraction, PVAS

I. INTRODUCTION

The fast growing technology and revolution in globalization of business, a strong reliable, high secure, authenticating system/human and for communication to carry valuable data in all sectors is very much necessary. For these purpose technology demands for a strong key/specialized system, that relays on safe transaction of data. One well-known method of authentication of human beings as well as data securing is by using biometric system. Contactless palm vein biometric is an automated technique to identify an individual [1]-[3]. The goal of proposed work is to design, develop, and secure authentication system using the present and upcoming biometric technology. The present work mainly deals with authentication by using contactless palm vein pattern [8], as it provides a complex vein patterns. Our focus here is on improving the security and performance of palm vein pattern, which is a popular biometric cryptosystem [14], [17]. Palm vein pattern can effectively utilize the natural representation of palm vein minutiae, which is an unordered set [4], [9]. The work provides a 2-way protection to the authentication system. This

technique provides, a high degree of accuracy, secure access, eco-friendly and new way of innovation.

II. RELATED WORK

It is necessary to realize and implement on hardware platform in order to improve accuracy and time compare to the software platform [11]. Many researchers worked on PV image feature detection, image enhancement and classification [1]. Nevertheless, in my survey authentication system development on proposed work is very less. This method is very simple and more reliable. Some papers also discussed about the multimodal PVAS, but these works did not show much effective result because of longer duration for recognition since it involves two modes of feature extractions steps [10]. Therefore, it is better to choose single mode to speedup the recognition process and for more secure we are providing secret key, which will not take much time to execute. In the present novel method, introduction to hardware implementation will test the suitability of palm features on FPGA platform and test the percentage of palm vein features accuracy on hardware platform. A 16-bit secret key is introducing to make PVAS more reliable and powerful authentication system. The Palm vein minutiae and secrete key data process on hardware requires encoding and decoding steps. Here to ensure secure encoding and decoding operations an intensive CRC polynomial construction approach is adopting.

Our first work [13] developed is based on real-time image using a CMOS sensor and that has to be pre-processed, finally features extracted and matched. This work did not produce expected output in terms of thinning, edge detection due to improper image acquisition. Because of this, we have chosen PUT standard database from institute of Control and Information Engineering (CIE) Biometrics for research purpose. For our present work, the database of contactless palm vein is taken from the PUT database [19]. PUT Vein pattern database is freely available for research purposes used as common platform for analysis, to study and comparison of new segmentation and classification algorithms. Enabling comparison of algorithms check with or without different hardware systems used by researchers will help us to choose the best algorithm, thus helping in biometrics systems design also.

III. BACKGROUND

Palm vein pattern or structure is unique from one individuals to other [5]. This uniqueness makes vein recognition system to more reliable system among different biometric modalities. The palm vein features security is enhancing by adding some crypt key [16]. The images taken from the database will be an input for the system. Before feature extraction process, the images are subjected to pre-processing using several techniques (will be describing in the following sections) [2]. After pre-processing the feature extraction based on centre-line thinning and gray value threshold, palm vein valid minutia points are extracting. These extract points are in 2D form. First, this must be converting into 1D values and fusion with the secret key. These set of values are further evaluating on FPGA for validation of data. To ensure proper encoding and decoding, error-detecting techniques called CRC algorithm is employing here. This algorithm proved that is very efficient method for validation of data without appending any error at the decoding stage [1]-[3].

A. CCITT - CRC

A 16-bit CRC the CCITT (*Committee Consultative International Tegrannique and Telephonique*) has the polynomial $x^{16} + x^{12} + x^5 + 1$, that is used as a 16-bit CRC checksum. The CCITT-CRC does not impose any additional transmission overhead at the character level. The data is considered as a binary number. Both sender and receiver need to divide the data using the same divisor. Then the quotient is discarding and the remainder is considered as the CRC. If the received data is errorless, then the receiver's data will match the sender's data, and the CRC's will agree. This checksum will ensure a secure data transmission.

B. Methodology

The proposed novel approach is analyzing in two models: software model and hardware model as shown in Fig. 1. The software model will perform, image preprocessing and minutiae extraction process and hardware model will check the validity of the process.

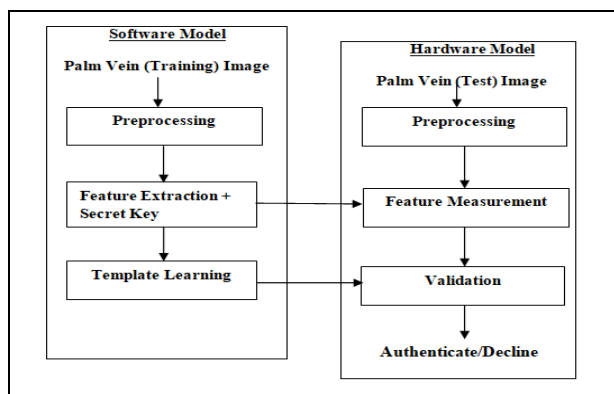


Fig.1 Proposed model of Authentication system

The complete flow of the proposed system is start with image preprocessing. Fig. 2 describes the preprocessing steps employed in the present work. After preprocessing the feature extraction process on enhanced image is applying. Once the

features extracted then the secret key generation process will start. Finally, the fusion of feature extracted, secret key data, will be carried, and the fusion data should be encoded for verification. Since all authentication system must be test in real time application, it is necessary to check on embedded system. To do so, here we are implementing and checking the system performance on hardware to validate the system accuracy and efficiency. The encoding and decoding operation will be developing on FPGA(Xilinx). During encoding process, the secret key and palm vein features both combined and the resultant data is encoded. At the decoding process, the data checked for genuine user palm. If the password and features match with the excepted data then the authentication is accepted else, authentication will be declining.

C. Palm Vein Preprocessing And Feature Extraction

Preprocessing reduces the noisy and inconsistent data. This section consists of around maximum 25 pixels. Preprocessing will eliminates all unwanted pixels.

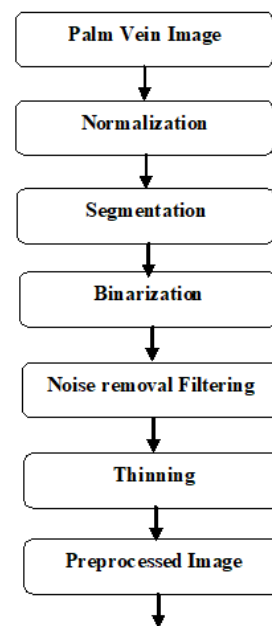


Fig.2 Preprocessing steps

Image normalization The linear normalization of a gray level image finding by,

$$I_N = (I - Min) \frac{newMax - newMin}{Max - Min} + newMin$$

Where I is an original palm vein image, Min is image minimum gray level, Max is image maximum gray level and $newMin$ and $newMax$ are after transformed min and max values respectively.

Image Segmentation We considered Threshold Segmentation i.e. *region-based segmentation*. The image is divided into two regions namely object region where the threshold is fixed to >160 gray values and background <160 . This is a type of global threshold.

Image Binarization. We applied *Recursive Otsu method*. The algorithm thoroughly searches for the threshold that

minimizes the intra-class variance. Therefore, the weighted sum of variances of the two classes defined by,

$$\sigma_{\omega}^2(t) = \omega_0(t)\sigma_0^2(t) + \omega_1(t)\sigma_1^2(t)$$

Where,

ω_0, ω_1 = two classes probabilities and threshold $t=160$

σ_0^2, σ_1^2 = two classes variance.

Noise Elimination is a process to remove redundant data in an image. Image averaging or smoothing is the best method for noise elimination. The *Gaussian filter* is success in this process and developed by,

$$g(x,y) = \exp\left(-\frac{x^2 + y^2}{2\sigma^2}\right)$$

Where, $g(x,y)$ is he processed image and $\sigma=2.5$ determines amount of smoothing.

Image Thinning. This process is also called as *skeletonization* [20]. In our observation, the *central line-thinning algorithm* [19] produces best-thinned image. Central line thinning algorithm (CLTA) calculated by the formula,

$$C_n = \sum_{k \in S} N_k - (N_k \cdot N_{K+1} \cdot N_{K+2})$$

Where,

N_k = intensity of the eight neighbors of the pixel,

N_0 = centre pixel

N_1 = intensity of the pixel to the right of the central pixel and the remaining are numbered in anticlockwise order around the centre.

Feature Extraction once the preprocessing is complete then the data is ready for feature detection and extraction process as shown in Fig. 3. The preprocessed image is well suited for feature extraction by removing of all noises present in the image.

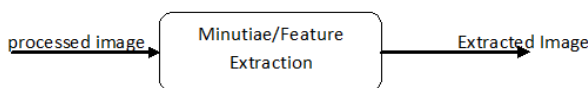


Fig.3 Block Diagram of Feature (Minutiae) Extraction

Palm vein feature detection and extraction process is a process of fine-tuning of the thinned image. Here we are using the crossing numbers approach as a feature-matching algorithm [12]. The algorithm operation is explaining in four steps.

1. First select a template of 3 x 3 pixels.
2. Next, using Euclidean distance find the pixels nearest Neighborhoods.

3. Find the overlapped pixels. If the number of overlapped pixels equals to two then that conveys beginning or end of the line. If the overlapped pixel equals to four and five then the bifurcation.

4. Pixels extracted from step 3 are considered as genuine minutiae points for authentication process.

D. Creating Secret Key And Crypt

The palm vein biometric systems are very hygienic and non-forgable method. The method to develop such strong system involves creating secret key and efficient crypt [21]. The palm vein template acts as a key. In the current implementation, the secret key 'S' generate 128-bit random bit stream. Hence the vein authentication system posses the secret key 'S' and the key is locked by the unordered set 'L' from the vein pattern. The polynomial 'P' is possessed by encoding key 'S' and 'L'. A crypt 'V' is developed by,

$$V = L \cup C$$

The V will secure 'S' with palm vein features. The chaff point set 'C' conceals the true set from the opponent. Concealing true set secures the secret feature set of the vein and template 'T'. In order to unlock Vault 'V', a query template 'T' is used. The 'T' is constructed by another unordered set say 'L¹'. The polynomial P is effectively reconstruct by overlapping 'L¹' with 'L', if both unordered set matches then the key is decoded.

E. Template Creation

In our work 'S' is considered as a data to be shield. The size of 'S' is based on system capacity. Here, we employed 8-bit length x and y coordinate values of the image feature extracted points as an image template (total length of template is 16-bit) is taken for locking/unlocking the vault.

IV. IMPLEMENTATION

The system implementations on FPGA, starts with an arrangement of image features that suit the translation and rotation between template and query feature data. Next, the encoding operation is carried to secure 'S' with palm vein feature data. If query features set similar to the template features set, then that indicates the authorized person presence and 'S' can be rebuild precisely.

Fig. 4 explains the complete system design flow of the proposed work, CRC-algorithm implementation process. Also describes the process of encoding and decoding operation. Appending the CRC bits to the original secret S (128-bits) and considerable image minutiae points of 16-bit from (x, y) coordinates of palm vein image total 144-bit data has been constructed as secrete CRC 'SC'.

A. Encoding Process Steps

Here the palm vein minutia has and secrete key values encoded. The following steps explain the encoding steps and realization of the system.

- (a) Secret Key: User password is 16-bit in length (includes both numbers and characters), guessing the password is

difficult for the opponents. The secret key then under goes a 16-bit CRC encoding using CCITT algorithm.

(b) CRC Coding and lock matrix creation: The computed CRC value is concatenating with secret key 'S' to form new secret key 'S¹'. Using Horner's methodology the vein features are select from the x-coordinate and the y-coordinates. The x and y-coordinate values are stored in matrix form that we called as the lock matrix.

(c) Chaff point Generation: This step ensures that the chaff point covers the entire pattern except the lock matrix coordinates.

(d) Vein pattern creation: The combination of chaff point and matrix coordinates forms the pattern. These patterns act as a secure template and therefore these values are stored in database.

B. Decoding Process Steps

Decoding process is for validation of the data. The following steps explain the process of decoding data.

(a) Polynomial Reconstruction: Based on unlock matrix the user Polynomial is reconstructed from polynomial interpolation method. To find all possible user polynomial, the unlock matrix is evaluated repeatedly.

(c) Interpolation: To rebuild the key locked among the vascular pattern, the features in the unlocking set must use interpolate polynomial.

(d) Polynomial Decoding: This step tells when all polynomial coefficients concatenated to form secret 'S¹'

(e) Error Detection: For all possible 'S¹', the CRC values computed and tally with the last 16-bits. Suppose CRC and last 16-bits is match then 'S¹' identified successfully.

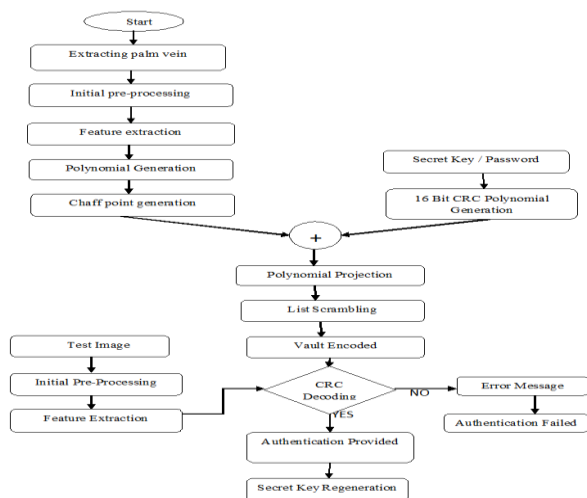


Fig.4 Proposed System Design flow

V. RESULTS AND DISCUSSION

The 600 left palm vein images from PUT Vein pattern database [18] is used to assess the proposed work. All palm images are 24-bit bitmap files with pixel dimensions of 1280x960 resolutions. For each individual, all sample images

were acquired in 3 series and 4 pictures per series. The time interval between each series was at least one week. In his device, there were no additional positioning systems used because the alignment of the device is in such a way that the volunteers were asked to put his/her hand on the device to cover capturing window so the line below their fingers coincident with its edge.

A. Preprocessing

Fig. 5 shows the simulation results of pre-processing and final minute extracted image result. Fig. 5(a) is the original image means that should be pre-processed. Images have been taken from the PUT standard palm vein database and cropped it for the region of interest 256*256 size. We can process an image without crop. Here to highlight the vein structure we have considered the cropped image. Fig. 5(b) depicts the image segmentation process of the palm image. Fig. 5(c) depicts the binarization process applied on Fig. 5(b) and Fig. 5(d) shows the noise elimination process applied to Fig. 5(c).

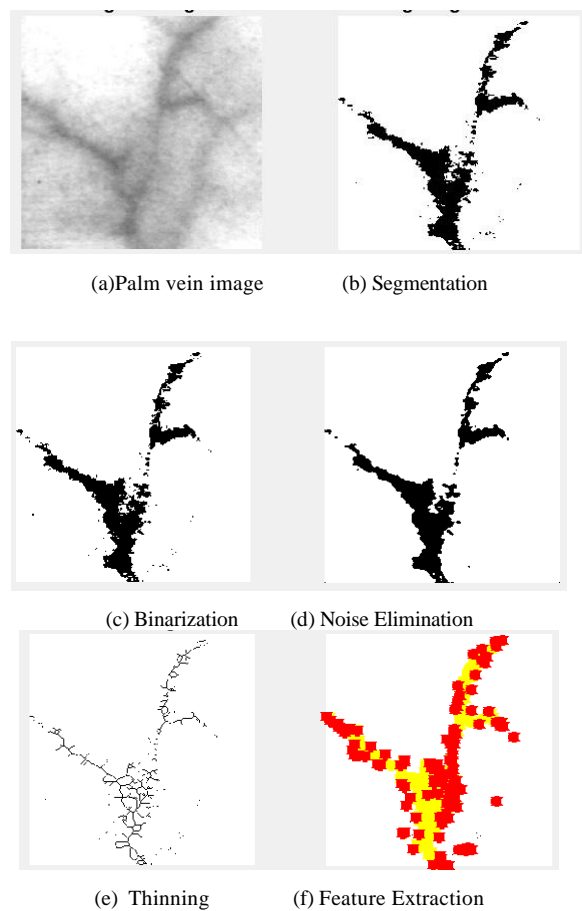


Fig. 5. Simulation Result

Fig. 5(e) shows the thinning process results from Fig. 5(d) and Fig. 5(f) is the feature-extracted image from the processed palm vein image. Final image concluded that there are more than 28 valid points (red color) are extracted and chaff points (yellow) is obtained. Fig. 6 shows valid minutiae's (features) extracted from an image. There are 144 different possible gray values in an image but only 42 are fair enough to recognize the image. These values are act as an image template for further process.

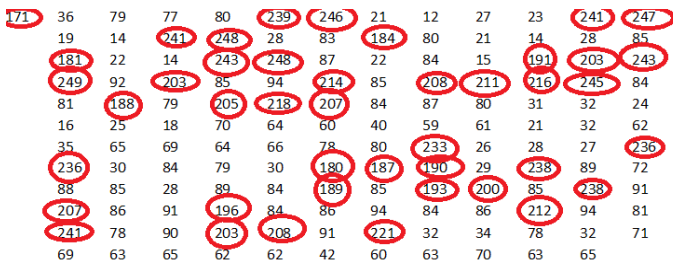


Fig. 6 Valid minutiae points of palm vein image (marked gray value for threshold >160)

We also run these extracted features for recognition process in MATLAB we got an accuracy of 98.16% and time taken for recognition out of 600 images is 1.235s as shown in table.1. For experimental purpose, we choose 600 images (only left hand of the persons) from the database.

B. Simulation On FPGA

1. After pre-processing and feature extraction, a minimum 28 valid minutiae points are selected (here the threshold is 160 gray value. If minute value is greater than 160 that is considered as valid minute points) and the input secret text 16 character as a secret code is entered by the user. Later the implementation process starts by construction of polynomial for secret key. This process is simulating on Xilinx ISE Design Suite 13.2: Vertex®-7 tools

2. The secret code is of 16- bit length. Development of CRC-16 algorithm on FPGA proves that the proposed system works well in identifying the genuine palm data without any error. Fig. 7. explains the device utilization by the system. One thing we conclude from this summary is that since to build entire system on hardware it requires only few logic devices. This will makes the system to occupy less area here by achieving high speed and improving other performance parameters such as power, cost etc. Therefore, the total time taken to complete the execution of the proposed system is 1.964ns that remarks the robustness of the system responds to an input which implemented on FPGA rather than Mat lab it takes 1.235s as mentioned in table. 1. The accuracy of the system build on FPGA is 98.921% out of 600 images as illustrated in table.1 and Fig. 8.

Device Utilization Summary				
Logic Utilization	Used	Available	Utilization	Note(s)
Number of Slice Flip Flops	16	10,944	1%	
Number of 4 input LUTs	178	10,944	1%	
Number of occupied Slices	94	5,472	1%	
Number of Slices containing only related logic	94	94	100%	
Number of Slices containing unrelated logic	0	94	0%	
Total Number of 4 input LUTs	178	10,944	1%	
Number of bonded IOBs	147	240	61%	
Number of BUFG/BUFGCTRLs	1	32	3%	
Number used as BUFGs	1			
Average Fanout of Non-Clock Nets	2.18			

Fig. 7 Device utilization summary

Table. I Comparison of result between software and hardware platform

Platform	Accuracy	Time
Software(MATLAB)	98.167%	1.235s
Hardware(FPGA)	98.921%	1.964ns

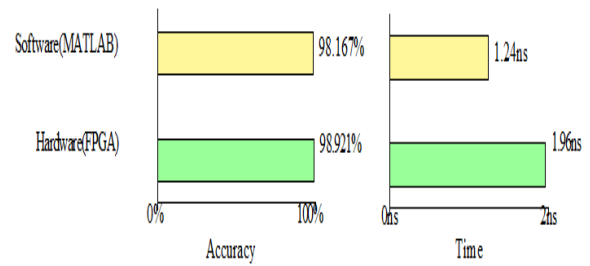


Fig. 8 Accuracy and Time Attributes Achieved

V1 CONCLUSION

A contactless palm vein feature extraction and realization on hardware platform is successfully tested and the best results are obtained. The system found effective and reliable when compare to the Matlab implementation. The system validation time found to be 0.964ns for proposed method when compared to 1.235s using Mat lab. Therefore, the system developed proves with a highly robust, high throughput of 1.964ns 2-level protection in terms of 16- bit secret key and the palm vein feature points matching.

REFERENCES

- Mr. Saagar Mukhopadhyay, Samir Kumar Bandyo padhyay "Palm Vein Authentication using Image classification Technique" *Journal for Research*, Volume 03, Issue 04, June 2017.
- Shriram D Raut et al "Development of biometric palm vein trait based person recognition system" *IEEE*, 978-1-5090-424-7/17, March 2017.
- Sonali Valid et al "Comparative Analysis of palm-vein recognition system using basic transforms" *IEEE*, 978-1-4799-8047-5/15, December 2015.
- Daniel Hartung, Martin Aastrup Olsen, et al "Spectral Minutiae for Vein Pattern Recognition", *Biometrics (IJCB)IEEE Conference*, 2011.
- Herry Setiawan and Eko Mulyanto Yuniarno "Features Extraction of Palm Vein Image Using Phase Symmetry" *International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME)*, Bandung, November 2-3 2015.
- Kama Nat Mishap, Kinder Aryan Mishap "Veins Based Personal Identification Systems: a Review", *I.J. Intelligent Systems and Applications*, No.10, pp.68-85, October 2016.
- M. Al-Juror, X. Wu, et al "Biometric Authentication System Based on Palm Vein", *International Conference Computer Science Applications*, pp. 52–58, 2013.
- G. K. O. Michael, T. Connie and A. T. B. Jin, "A preliminary acclimatization study of a contactless biometrics using palm vein feature", *IEEE Conference Industrial Electronics Application*, pp. 1022–1027, 2011.
- L. Wang, G. Leedham, and D.S. Cho. "Minutiae feature analysis for infrared hand vein pattern biometrics", *Pattern Recognition*, Vol.41, No. 3, pp. 920-929, 2008.
- Y. Zhou and A. Kumar, "Human identification using palm-vein images", *IEEE Transaction Information Forensics Security*, Vol. 6, No. 4, pp. 1259– 1274, 2011.
- M. Alareqi, K. Mateur, R. Elgouri and L. Hou, "FPGA Based Image Processing Algorithms (Digital image enhancement techniques) using Xilinx system generator", *European Journal of Scientific Research*, Vol. 134, No. 3, pp. 336-346, 2015.
- Dorota Smorawa "Verification of people based on plam vein with the ROI automatic appointment", *Journal of applied mathematics and Computational mechanics*, Vol.15, No.3, 123-133, 2016.
- A. Ross and A. Jain, "Information fusion in biometric", *Pattern Recognition Letters*, vol. 24, pp. 2115–2125, 2003.

- [14] Keerthi C, A.P.Savitha et al, "A Robust Palm Vein Authentication for Improving Safety and Security", *International Journal of Innovative Research in Computer Science & Technology (IJIRCST)*, ISSN: 347-5552, Vol.3, No.3, May-2015.
- [15] Yuhang Ding, Dayan Zhuang, and Kejun Wang, "A Study of Hand Vein Recognition Method", *IEEE International Conference on Mechatronics & Automation*, pp.2106-2110, July 2005.
- [16] Anil K. Jain, Arun Ross and Salil Prabhakar, "An Introduction to Biometric Recognition", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 14, No.1, pp. 4-20, July 2005.
- [17] Rabia Bakhteri. "Biometric encryption using finger print fuzzy vault for FPGA-based embedded systems", *IEEE Conference- TENCN*, 2009.
- [18] Control and information engineering institute.
<http://www.cie.put.poznan.pl>.
- [19] http://www.eng.fiu.edu/me/robotics/elib/am_st_fiu_ppr_2000.pdf
- [20] <http://www.inf.u/~palagyi/skel/skel.html#Applications>